

REMARKS

Claims 1-19 and 24-27 were pending and rejected in an Office Action dated August 6, 2008.

Claims 3, 14, 24, 26, and 27 are amended, claims 1-2 and 5 are canceled, and claim 28 is added.

Claims 3-4, 6-19, and 24-28 are pending upon entry of this amendment. In view of the Amendments herein and the Remarks that follow, Applicant respectfully requests that Examiner reconsider all outstanding rejections, and withdraw them.

Response to Rejections Under 35 USC § 102

In the Office Action, the Examiner rejected claims 1-4, 14-19, and 24-27 under 35 USC § 102. Claims 1-3 and 24-26 were rejected as being anticipated by U.S. Patent No. 6,230,288 ("Kuo"). Claims 1-4, 14-19, and 24-26 were rejected as being anticipated by U.S. Patent Publication No. 2005/0028002 ("Christodorescu"). Claim 27 was rejected as being anticipated by U.S. Patent No. 7,266,844 ("Teblyashkin"). These rejections are respectfully traversed with respect to the claims as amended.

Claim 1-2 are canceled, and therefore the rejections of these claims are overcome. Claims 3-4, 14-19, and 27 are amended to depend on claim 6. As mentioned by the Examiner, Christodorescu does not disclose all of the elements of claim 6. Also, Kuo does not anticipate claim 6. Kuo discloses a method for detecting computer viruses that infect text-based files by transforming whitespace within the text-based files. Kuo does not mention computer code having a decryption loop and a body. In addition, Teblyashkin does not anticipate claim 6. Teblyashkin discloses computer viruses based on redundancy in viral

code. Teblyashkin does not disclose optimizing code. Claim 24, as amended, contains similar language to claim 6. As a result, claims 3-4, 14-19, and 24-27 are not anticipated by Christodorescu, Kuo, or Teblyashkin. Therefore, Applicant respectfully requests that Examiner reconsider the rejections and withdraw them.

Response to Rejections Under 35 USC 103(a)

In the Office Action, the Examiner rejected claims 5-13 under 35 USC § 103(a) as being unpatentable over Christodorescu in view of U.S. Patent No. 5,826,013 (“Nachenberg”). This rejection is respectfully traversed.

Claim 6 recites a computer-implemented method for determining whether computer code contains malicious code, the method comprising:

identifying computer code suspected of currently containing malicious code, the computer code having a decryption loop and a body;
optimizing the decryption loop to produce optimized loop code;
performing a malicious code detection procedure on the optimized loop code;
optimizing the body to produce optimized body code;
subjecting the optimized body code to a malicious code detection protocol; and
responsive to the malicious code detection procedure detecting malicious code in the optimized loop code or the malicious code detection protocol detecting malicious code in the optimized body code, declaring a confirmation that the computer code contains malicious code.
(emphasis added)

As can be seen, claim 6 recites identifying computer code suspected of currently containing malicious code, where the computer code has a decryption loop and a body. The decryption loop is optimized to produce optimized loop code and a malicious code detection procedure is performed on the optimized loop code. A confirmation of malicious code is

declared responsive to detecting malicious code in the optimized loop code or in optimized body code. By optimizing the decryption loop, the claimed invention beneficially removes possible obfuscations in the decryption loop so that a malicious code detection procedure can be more efficient and successful. The optimization can also result in faster emulation of the decryption loop to decrypt the body of the computer code. Support in the specification is found, for example, on page 4, line 16 to page 5, line 21 and on page 10, lines 21-27.

Claim 6 is not obvious in view of Christodorescu and Nachenberg. Christodorescu discloses converting a program to a “standardized version” that expresses the function of the program and using this standardized version for malware detection. Nachenberg describes a method for detecting a polymorphic virus using emulation, similar to the method described in the Background Art of the present specification. Applicant has previously discussed several portions of Nachenberg in remarks filed with an amendment on January 22, 2008, and with a pre-appeal request for review on February 20, 2008.

The references do not show “optimizing the decryption loop to produce optimized loop code,” or “performing a malicious code detection procedure on the optimized loop code.” The Examiner cites Nachenberg, col. 1, lines 63-67, and col. 2, lines 1-25, and Christodorescu, paragraph [0011], as disclosing each of these elements. However, the cited portions of Nachenberg merely describe examining sequences of instructions **during emulation** to determine if those sequences are likely part of a decryption loop (e.g., the sequences contain “boosters”). The cited portion of Christodorescu discloses creating a standardized version of a program and comparing the standardized version to standardized malicious code portions. Neither portion discloses optimizing a decryption loop and performing a malicious code detection procedure on the optimized code.

Based on the above remarks, Applicant submits that for at least these reasons a person of ordinary skill in the art would not find the invention as defined in claim 6 or dependent claims 7-13 to be obvious over the cited references. Therefore, Applicant respectfully requests that the Examiner reconsider the rejection and withdraw it.

Claim 9, dependent on claim 6, recites “wherein the step of optimizing the body comprises using at least one output from the group of steps consisting of optimizing the decryption loop and performing a malicious code detection procedure on the optimized loop code.” The Examiner cites Christodorescu, paragraph [0011], and Nachenberg, col. 3, lines 35-53, as disclosing this element. However, the cited portion of Nachenberg merely discloses emulating (rather than optimizing) a possible decryption loop and scanning the virus body after sufficient emulation. The cited portion of Christodorescu is discussed above.

Claim 10, dependent on claim 6, recites “wherein, when the step of performing a malicious code detection procedure on the optimized loop code indicates the presence of malicious code in the computer code, the steps of optimizing the body and subjecting the optimized body code to a malicious code detection protocol are aborted.” The Examiner cites Christodorescu, paragraph [0031], as disclosing this element. However, this portion merely discloses outputting a representation of a malicious code portion when such a portion is present.

Claim 11, dependent on claim 6, recites “further comprising the additional step of, after the step of performing a malicious code detection procedure on the optimized loop code, revealing an encrypted body.” Claim 12, dependent on claim 11, recites “wherein the step of revealing an encrypted body comprises emulating the optimized loop code.” The

Examiner cites Nachenberg, col. 6, lines 10-31 as disclosing these elements. However, the cited portion of Nachenberg merely discloses emulating instructions to allow a polymorphic virus to decrypt itself. These emulated instructions have not been optimized and have not been previously subjected to a malicious code detection procedure.

Claim 14, dependent on claim 6, recites “performing a backward pass operation.” The Examiner cites paragraphs [0018] and [0021] of Christodorescu as disclosing this element. However, the cited portions do not mention a backward pass portion of an optimization.

Applicant is adding new claim 28. Applicant asserts that this claim is supported by the specification and is not anticipated or obvious in view of any of the references discussed above.

Applicant invites Examiner to contact Applicant’s representative at the number provided below if Examiner believes it will help expedite furtherance of this application.

Respectfully Submitted,
Frederic Perriot

Date: November 5, 2008

By: /Nikhil Iyengar/

Nikhil Iyengar, Reg. No. 60,910
Attorney for Applicant
Fenwick & West LLP
801 California Street
Mountain View, CA 94041
Tel.: (415) 875-2367
Fax: (650) 938-5200